Warnings against extortion under threat of DDoS attacks

Threats of denial of services attacks associated with ransom demands (RDDoS) faced by French companies since August 2020 seem to be part of an extorsion campaign that began around October 2019. The lucrative aim of this campaign is undeniable, although a secondary objective of destabilization can be envisaged, given for example the targeting of market infrastructures whose continuity of activity is critical.

Observed Phenomenon: the receipt of threatening e-mails
In recent threats that have been observed by CERT-FR, the target receives an e-mail in which the sender claims to belong to attacker groups or APT like APT28, APT29, Lazarus, Armada Collective, Carbanak, Anonymous or Silence. He informs his recipient that his website or network will be targeted by the next DDoS attack of the group, from a date specified to him.

To reinforce the intimidation effect, the group of attackers carries out a demonstration DDoS attack that targets the victim’s back end infrastructure, APIs and DNS servers, which can cause greater difficulties than traditional DDoS on websites.

Although attackers claim to be able to reach peaks at 2 terabits per second, no volume greater than 150 gigabits per second has been reported to ANSSI during demonstration DDoS attacks. In open sources, at the time of writing this bulletin, this volume does not exceed 200 gigabits.

Example of an observed email:

We are the Lazarus and we have chosen [VICTIME] as target for our next DDoS attack.

Please perform a google search for « Lazurus Group » to have a look at some of our previous work.

Also, perform a search for « NZX » or « New Zealand Stock Exchange » in the news. You don’t want to be like them, do you?

Your whole network will be subject to a DDoS attack starting in 7 days at [REDACTED] next week. (This is not a hoax, and to prove it right now we will start a small attack on a few of your unimportant IPs in [REDACTED] range that will last for 30 minutes. It will not be heavy attack, and will not cause you any damage, so don’t worry at this moment.)

There’s no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps)

What does this mean? This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers.

You will lose Internet access in your offices too, probably.

How you can stop this? We will refrain from attacking your servers for a small fee. The current fee is 20 Bitcoin (BTC). It’s a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don’t have it already.

If you don’t pay attack will start, fee to stop will increase to 30 BTC and will increase by 10 Bitcoin for each day after deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: [REDACTED]
Once you have paid we will automatically get informed that it was your payment.

Please note that you have to make payment before the deadline or the attack WILL start!

What if you don’t pay?

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

Do not reply to this email, don’t try to reason or negotiate, we will not read any replies. Once you have paid we won’t start the attack and you will never hear from us again. Please note that no one will find out that you have complied.

Nonetheless, it should be noted that this email is only an example, and even if it is representative of a number of recent extortion threats, it is not necessarily representative of all threats encountered.

A threat that would not be followed by facts

This phenomenon, also detected by other organizations, is carried out by a group, a priori of a cybercriminal nature. These threats are similar to a scam to the extent that none of those observed have been executed and therefore followed by action in case of non-payment.

Moreover, attackers would not be able to distinguish between victims who paid the ransom and those who ignored the extortion. Indeed, Bitcoin ensures the anonymity of the transactions and a single Bitcoin address is reused in several emails sent to different targets.

This practice, however, would have allowed the scammers to amass several hundred thousand dollars from the victims of blackmail, although the threats of which ANSSI has become aware have not been executed to date.

CERT-FR’s recommendations

In general, CERT-FR recommends not to give in to blackmail and therefore not to pay the ransom demanded, regardless of the extortion method used by the attacker (DDoS, ransom…). More specifically, with regard to threats of DDoS attacks, the reasons are as follows:

- there is no guarantee that the payment of the ransom will effectively prevent or stop an attack;
- nothing proves that the scammers have the capacity to carry out their threat, especially if no attack has been carried out at the time of the ransom demand;
- this encourages the development of this type of scam, especially against victims who have agreed to pay in the past and who will potentially still accept if a new threat arises;
- it helps finance the groups behind the scam and thus strengthen their infrastructure to carry out larger-scale attacks later.
Similarly, CERT-FR advises against replying to threatening emails and possible following reminders. Indeed, this would confirm the validity of the targeted e-mail address and could incite perpetrators to increase the pressure on their victim.

The target of such a threat, on the other hand, can prepare for the possibility of an imminent attack by implementing appropriate measures to protect themselves. A guide available on the website of ANSSI (French National Cybersecurity Agency) recalls the measures to be taken to protect oneself and react to a DDoS attack (see Documentation).

Documentation


Rappel des avis émis

Dans la période du 07 au 13 septembre 2020, le CERT-FR a émis les publications suivantes :

- **CERTFR-2020-ALE-019** : Recrudescence d’activité Emotet en France
- **CERTFR-2020-AVI-548** : Multiples vulnérabilités dans le noyau Linux de SUSE
- **CERTFR-2020-AVI-549** : Multiples vulnérabilités dans les produits SAP
- **CERTFR-2020-AVI-550** : [SCADA] Multiples vulnérabilités dans les produits Siemens
- **CERTFR-2020-AVI-551** : [SCADA] Multiples vulnérabilités dans Schneider Electric SCADAPack
- **CERTFR-2020-AVI-552** : Vulnérabilité dans le noyau Linux d’Ubuntu
- **CERTFR-2020-AVI-553** : Multiples vulnérabilités dans le noyau Linux de SUSE
- **CERTFR-2020-AVI-554** : Multiples vulnérabilités dans Google Android
- **CERTFR-2020-AVI-555** : Vulnérabilité dans Citrix StoreFront
- **CERTFR-2020-AVI-556** : Multiples vulnérabilités dans Google Chrome
- **CERTFR-2020-AVI-557** : Multiples vulnérabilités dans les produits Intel
- **CERTFR-2020-AVI-558** : Vulnérabilité dans F5 BIG-IP
- **CERTFR-2020-AVI-559** : Multiples vulnérabilités dans Microsoft IE
- **CERTFR-2020-AVI-560** : Multiples vulnérabilités dans Microsoft Edge
- **CERTFR-2020-AVI-561** : Multiples vulnérabilités dans Microsoft Office
- **CERTFR-2020-AVI-562** : Multiples vulnérabilités dans Microsoft Windows
- **CERTFR-2020-AVI-563** : Vulnérabilité dans Microsoft .Net
- **CERTFR-2020-AVI-564** : Multiples vulnérabilités dans les produits Microsoft
- **CERTFR-2020-AVI-565** : Vulnérabilité dans OpenSSL
- **CERTFR-2020-AVI-566** : Multiples vulnérabilités dans Palo Alto Networks PAN-OS
- **CERTFR-2020-AVI-567** : Vulnérabilité dans Ruby on Rails
- **CERTFR-2020-AVI-568** : Multiples vulnérabilités dans le noyau Linux de SUSE

Gestion détaillée du document
le 16 septembre 2020
Version initiale
le 17 septembre 2020
changed flag into (EN) for english

Conditions d’utilisation de ce document : https://www.cert.ssi.gouv.fr
Dernière version de ce document : https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-007/